Privacy Impact Assessment for the VA IT System called:

**Burial Operations Support Systems Enterprise (BOSS-E)** Amazon Web Services (AWS)

**National Cemetery Administration (NCA)**

Date PIA submitted for review:
02-18-2022

System Contacts:

<table>
<thead>
<tr>
<th>Title</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Lakisha Wright</td>
<td><a href="mailto:Lakishia.Wright@va.gov">Lakishia.Wright@va.gov</a></td>
<td>202-632-7216</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Karen McQuaid</td>
<td><a href="mailto:Karen.McQuaid@va.gov">Karen.McQuaid@va.gov</a></td>
<td>708-724-2761</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Michael Ouslander</td>
<td><a href="mailto:Michael.Ouslander@va.gov">Michael.Ouslander@va.gov</a></td>
<td>202-891-9710</td>
</tr>
</tbody>
</table>
Abstract

The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.

As authorized under the National Cemeteries Act of 1973, the Memorial Benefits System (MBS) is a system enclave consisting of two major components, Burial Operations Support System/Automated Monument Application System (BOSS and AMAS) and several minor interdependent components that utilize common data to automate all business processes associated with monuments and interments.
Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The Memorial Benefits Application (MBS) is a Major Application hosted at the Quantico Information Technology Center (QITC) and managed by Infrastructure Operations (IO). The MBS serves customers in the National Cemetery Administration (NCA) and their partners, State/Tribal/Military Cemeteries to provide memorial benefits for Veterans and their families.

As authorized under the National Cemeteries Act of 1973, the MBS is an application enclave consisting of two primary components (BOSS and AMAS) and several other minor components that are interdependent and utilize common data.

The MBS is a Major IT investment according to the Office of Management and Budget (OMB). In accordance with OMB Circular A-11 and in the context of the Capital Planning and Investment Control (CPIC), all requirements applicable to the MBS are set forth in the OMB Exhibit 300.

The MBS is an Infrastructure Operations (IO) managed system, meaning that its entire infrastructure is supported by the IO service line structure. Each service line has a separate Federal Information Security Management Act (FISMA) accreditation boundary. Along with VA National, each service line functions as the security control provider for certain security controls. Implementation of the
security controls provided by each service line is documented in the respective system security plan for each IO Service Line.

Security controls specific to facilities management, the IO policy, infrastructure, and telecommunications are not part of the MBS Assessment and Authorization (A&A) accreditation boundary. Rather, they are the responsibility of VACO/NCA Facilities and the Enterprise Operations (EO), Data Center Operations (DCO), the Enterprise Infrastructure Support (EIS) - Windows Platform, the EIS - Unix Platform, and the IO Network Operations ITC (Telecom) Service Lines, respectively. The IO Service Lines are responsible for nearly $100 billion in Veteran benefits for the Department, as well as the National Cemetery Administration (NCA), Health (VHA), and Benefits (VBA) processing.

The following active components comprise the Memorial Benefits Application:

**Burial Operations Support Systems (BOSS):** BOSS was developed to provide benefits delivery automation support to National and State/Tribal Veteran and Military Cemeteries nationwide. BOSS automates the manual, paper intensive record keeping, information and forms processing associated with interments. Veteran Eligibility is usually determined by presentation of discharge papers (DD214) or other supporting documents. Such artifacts can be sent via secure fax to the MBS through the Memorial Enterprise FAX Service Re-Platforming (EFSR) system (a separate FISMA master system that connects securely to BOSS). Artifacts relevant to the case are stored digitally in the Management Application Scanning System (MASS) database. MASS is a commercial off-the-shelf (COTS) image management and repository solution called Feith. The images are indexed to the case and can be retrieved for subsequent viewing through AMAS and the Presidential Memorial Certificate (PMC). BOSS allows the National Cemetery Administration (NCA) to provide electronic transfer of information for the VA corporate master Veteran identification initiative. BOSS processes approximately 150,000 burial cases per year. The primary objective and programmatic need was to automate the manual, paper-intensive record keeping, information and forms processing associated with interments. BOSS provides the VA required nationwide burial location capabilities, date of death information, and links to gravesite reservation files; although the Master Person Index (MPI) is now used to manage First Notification of Death (FNOD) processing.

A BOSS application request is initiated by a validated customer from a National or State Veteran Cemetery. The process for entering a decedent into BOSS begins with a Record of Interment (ROI) input by cemetery personnel. During the application request process, data on the decedent and the interment are collected. The system user schedules the interment and initiates the order process for the headstone or marker. Once all information has been captured correctly, the ROI is approved by NCA staff. Once approved, the interment is placed on the schedule and the order is processed.

**Automated Monument Application System (AMAS):** AMAS was developed to automate all business processes associated with monument applications (i.e., ordering, delivering, and tracking). Through ongoing development of the automation, integration, and standardization of AMAS functions, the NCA can accommodate an increasing workload; maximize the utilization of personnel and physical resources; and capture information needed for the Memorial Program Service (MPS) and VA information resources management planning activities. AMAS processes approximately 360,000 applications (via VA Form 1330) for government-furnished monuments each year; including
headstones, markers, medallions, and niche covers. AMAS tracking capability expedites claims research and NCA’s subsequent response to case inquiries.

Requests for headstones and markers are initiated by funeral homes when the decedent is to be buried in a private cemetery. The funeral homes, with the assistance of the decedent’s family, fill out VA Form 1330, Application for Standard Government Headstone or Marker. This form is faxed (through the EFSR system) or mailed along with supporting documents (i.e., DD214 or other proof of eligibility) to the Memorial Program Service (MPS) office for processing. Once received by the MPS office, the form is scanned and bar-coded into the MASS database (Feith commercial-off-the-shelf (COTS) solution). Information captured and imaged from the Form 1330 is manually entered into the MBS Enterprise database application by MPS agents. The MPS agent opens the Form 1330 image and simultaneously opens the AMAS application to enter the monument application information. Once information is entered into AMAS, an absolute path to the scanned file (via bar-code) is entered to capture the link between the AMAS record and the stored file. The case is forwarded to an MPS Case Manager for approval. The Case Manager reviews the case and ensures that the decedent is eligible to receive a marker or headstone, and that all relevant information has been verified. Once the Case Manager grants approval, the case is then forwarded to the Centralized Contracting Division (CCD) for processing. The process for the completion and delivery of the headstone/marker is the same as that for Veterans being buried in a National Cemetery.

**Daily Cemetery Burial Schedule (DBS):** The goal of the DBS is to enable the public to view, through an Internet browser, relevant burial schedule information on persons being interred at a VA National Cemetery or State Veteran Cemetery that uses Burial Operations Support System (BOSS) for burial scheduling. This service is expected to reduce the number of inquiry phone calls to NCA, funeral homes, and VA cemeteries by offering a self-service tool for the public.

**Eligibility Office Automation Capability/Manual Pre-Need (EOAS):** The EOAS is a sub-component of the BOSS application that provides for the automation of the Eligibility Office functions. BOSS provides a workflow process for the cemetery, from the first contact with the funeral home, to checking eligibility, scheduling the interment, and ordering and setting the monument. The EOAS also provides an easy method for retrieval of historical record for interment.

**Web Presidential Memorial Certificate - Processing Capability (WebPMC):** A single PMC is automatically generated for a Veteran’s family, loved ones or next of kin when a Veteran burial is completed and entered into the Burial Operational Support System (BOSS). The BOSS program is used to support and help manage burials at VA National Cemeteries as well as most State Veteran Cemeteries. PMCs are also automatically generated and sent to the listed “Applicant” when a government furnished headstone, marker, or medallion is ordered using VA Form 40-1330, or VA Form 40-1330M.

The PMC system component of the MBS contains information on PMC records, whether created due to a burial in a National or State Veteran cemetery, created from an application for a marker or headstone, or requested by phone, email, fax, or sent via United States Postal Service mail. The PMCs received via fax are managed through MASS (Feith COTS Solution). The data from Veterans buried in a VA National or State Veteran Cemetery or a request for a marker or headstone are
compiled weekly through a routine that reviews the BOSS database and captures all necessary and associated information from Veteran burial records that can be used to generate a PMC.

**Kiosk/Grave Locator Service (KNGL):** The Kiosk/Nationwide Gravesite Locator (KNGL) system is a publicly accessible sub-component of the MBS used to conduct searches for Veteran and gravesite information within the cemetery system. In this case, a separate KNGL database extracts data from MBS databases within the VA enclave (protected by a firewall). The KNGL database itself is also protected through application partitioning, such that only the intended public portion (the interface) is in the demilitarized zone (DMZ) (outside the enclave boundary).

Extracts of the MBS information are also provided to the Nationwide Gravesite Locator, which is a web-based application available through the NCA website: [http://gravelocator.cem.va.gov/index.html](http://gravelocator.cem.va.gov/index.html)

The Nationwide Gravesite Locator includes burial records from many sources. These sources provide varied data; some searches may contain less information than others. Information on Veterans buried in private cemeteries is collected to furnish grave markers and has no information for burials prior to 1997. The data extracted for the Grave Locator Service is stored in the demilitarized zone (DMZ), which is a perimeter subnetwork that contains and exposes NCA external-facing services to the Internet. Since the service does not require identification and authentication, it has not been assigned an eAuthentication assurance level as described in the OMB Memorandum M-04-04. The DMZ exclusively contains read-only information; is public-facing; and contains no privacy or protected health information.

**Management and Decision Support System (MADSS):** The NCA Management and Decision Support System (MADSS) is an electronic system of tracking cemetery workload and administrative data. The MADSS was developed to improve the accuracy and consistency of data received from the national cemeteries. The information for MADSS is collected under the authority in title 38, United States Code, sections 2400(a) and 2404.

NCA/MADSS is a menu driven, user-friendly, online data entry system. Cemeteries submit workload and administrative data to the Department of Veterans Affairs (VA) Quantico Information Technology Center (QITC) in Virginia. Cemetery personnel can enter current month or quarterly data and correct current month or quarterly data within the current fiscal year. The system also gives the NCA Central Office, the Memorial Service Network (MSN) and national cemetery staff the ability to generate and print reports.

Information on Veterans buried in private cemeteries is collected to furnish grave markers and has no information for burials prior to 1997.
Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy-Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- [ ] Name
- [ ] Social Security Number
- [ ] Date of Birth
- [ ] Mother’s Maiden Name
- [ ] Personal Mailing Address
- [ ] Personal Phone Number(s)
- [ ] Personal Fax Number
- [ ] Personal Email Address
- [ ] Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- [ ] Financial Account Information
- [ ] Health Insurance Beneficiary Numbers
- [ ] Account numbers
- [ ] Certificate/License numbers
- [ ] Vehicle License Plate Number
- [ ] Internet Protocol (IP) Address Numbers
- [ ] Current Medications
- [ ] Previous Medical Records
- [ ] Race/Ethnicity
Veteran or primary subject - service information and benefit information for burial. Contact person for the decedent: name, relationship to Veteran, address and telephone number.

**PII Mapping of Components**

The Memorial Benefits System consists of two major components, BOSS and AMAS. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the Memorial Benefits System and the functions that collect it are mapped below.

**PII Mapped to Components**

*Note:* Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOSS</td>
<td>Yes</td>
<td>Name, SSN, DOB of decedent; contact info (address, phone, fax, email, SSN) for POC of Veteran or Veteran’s family member being buried</td>
<td>Memorial benefit delivery automation support</td>
<td>Database encryption and access control</td>
</tr>
</tbody>
</table>
### Database Name of the information system collecting/storing PII
Does this system collect PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/Storage of PII | Safeguards
--- | --- | --- | ---
AMAS | Yes | Name, SSN, DOB for decedent Veteran, contact info (address, phone, fax, email) of the POC for Veteran being buried | Processing application for monument (burial headstones) | Database encryption and access control

#### 1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators? Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The MBS-BOSS component receives data from funeral homes, next of kin, and other points of contact for the decedent for burial services. The AMAS component collects data directly from individuals as part of a monument application. Given the purpose of the Memorial Benefits System, the individuals for which the data is being collected are decedent Veterans or their deceased family members, so the information will always need to be collected on their behalf.

#### 1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?
If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number. This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The MBS does not receive information electronically from other systems. A long-term plan is in place for the Pre-Need system to transmit data electronically to the EOAS component of BOSS, but these activities are currently processed by scheduling office personnel. Documents from funeral homes, next of kin, and other points of contact from the decedent are sent to scheduling office personnel and uploaded into BOSS. AMAS processes approximately 360,000 claims for standard government headstones or markers (VA Form 40-1330) and Monument and Presidential Memorial Certificate Request (VA Form 40-0247) applications annually. Data from the forms are manually entered into the system. Forms and supporting documentation required to verify memorial benefits eligibility, such as the DD214, are scanned/uploaded.

What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

The MBS collects and maintains information to verify the identity and eligibility of the Veteran or decedent for burial and monument services.

1.4 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Data is manually verified by the Scheduling Office through Beneficiary Information Record Locator System (BIRLS) for accuracy. The information stored in the system is checked for accuracy by cross referencing the data with information available on DoD Forms 214 or other sources (e.g., data
received from previous benefit requests). Additionally, since the information is submitted directly from an individual, the information may be validated with the original source.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.

This question is related to privacy control AP-I, Authority to Collect.

The MBS operates under the following System of Record Notice (SORN):
48VA40B - Veterans (Deceased) Headstone or Marker Records-VA, per Title 38, United States Code: Sections 501(a), 501(b), and Chapter 24, Sections 2400-2404.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

* Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

* Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

* Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

* Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:** BOSS/AMAS collects the SPI on deceased Veterans and limited contact information from their next of kin/point of contact for arranging the burial. If this information were breached or accidentally released to inappropriate parties or the public, it could result in potential personal and/or
emotional harm to the friends/relatives of the individuals whose information is contained in the system.

**Mitigation:** The Department of Veterans Affairs is careful to only collect the information necessary to identify the recipients of memorial benefits and process their interment and memorial requests. This involves a review process to identify potential inconsistencies or other issues. By only collecting the minimum necessary information to process each request, VA can better protect the individual’s information. Records are only released to individuals authorized to coordinate interments on behalf of the deceased person (generally, the next of kin) upon receipt of proper identification.

VA applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation. NCA Information Security Officer is responsible for administering VA Information Security Programs at NCA facilities, to help them maintain compliance with federal security requirements and VA security policies. This operational security posture maintains and safeguards system information from threats.
Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program’s business purpose.

*Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.*

- Name: Used to verify Veteran or decedent’s identification. Also collect if subject is a contact person for decedent
- Social Security Number: Used to verify Veteran or subject’s identity
- Date of Birth: Needed for monument inscription
- Mailing Address: Collected for decedent’s POC
- Zip Code: Part of the mailing address
- Phone Number: Collected for decedent’s POC
- Fax Number: Collected for decedent’s POC
- Email Address: Collected for decedent’s POC
- Emergency Contact: Just the POC (not emergency)
- Service Information: Used to verify Veteran’s eligibility
- Benefit Information: Used to verify burial benefits
- Relationship to Veteran: Required when decedent is not the Veteran to determine eligibility

2.2 What types of tools are used to analyze data and what type of data may be produced?

*Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.*

*If the system creates or makes available new or previously un-utilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual’s existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*

*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.*

The MBS system itself does not perform any kind of analysis or run analytic tasks in the background.
2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?
Information is protected at rest through AES-256 encryption using AWS KMS secure server side, when stored in Oracle RDS and S3 buckets. Information is protected in transit through TLS 1.2 with an AES-256 cipher. The Oracle RDS database is located in a private subnet, protected by an AWS Security Group that allows access only from application servers and a bastion host in the same AWS VPC. So, it is not possible to connect directly to the database from outside the VPC.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
Access to SSNs are limited to those with a need-to-know via database authentication and role-based grants. SSNs are removed from communications and copies of data.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.
The following discusses what to do when spillage happens:

- How soon should you report the incident?
  - Always report any suspected incident immediately.
  - VA policy requires that incidents must be reported to the VA NSOC within one hour of being discovered or reported to their management, ISSO, or PO. This means your PM must be informed as soon as possible.
- Who do you report an incident to? To your project leads and manager.
- What if the incident occurs after hours or on a weekend? Notify your PM according to local emergency procedures and they will contact VA ISSO and VA chain of command.
- What information needs to be reported? Describe what happened, including who was involved, when it happened, what system was compromised, what information was revealed, and any other details that you have.
- What if you suspect unethical or malicious actions? Contact your PM, if possible. If not, use the Booz Allen Ethics hotline - 800-291-9955.

2.4 Privacy Impact Assessment: Use of the information.
How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project
covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

**Principle of Transparency:** Is the PIA and SORN, if applicable, clear about the uses of the information?

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a Veteran’s burial and monument benefits.

The security controls for the MBS application cover 18 security areas related to protection of the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; assessment, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The MBS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy and VA National Rules of Behavior in the Talent Management System govern how Veterans’ information is used, stored, and protected.
Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

- Name
- Social Security Number
- Date of Birth
- Mailing Address
- Zip Code:
- Phone Number
- Fax
- Email Address
- Emergency Contact
- Service Information
- Benefit Information
- Relationship to Veteran
- Military service data and name and address of individual
- Name and address of next-of-kin
- Military service data, applicant’s name and address, place of burial, burial services and headstone data

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

SORN 48VA40B: Retained indefinitely.
3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

The retention schedule has been approved by the VA records office and NARA. The retention schedule 1180.17 for Veterans Benefits indicates to “Cutoff after receipt of last relevant correspondence. Transfer to NARA 50 years after cutoff.”

Records Control Schedule 10-1 (va.gov)

The SORN for the MBS system is as follows:

48VA40B - Veterans (Deceased) Headstone or Marker Records

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.?

This question is related to privacy control DM-2, Data Retention and Disposal.

Paper records are destroyed upon manual entry into the MBS; this is an NCA business process external to the MBS system. Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization. Once entered into the electronic system, records in the MBS are stored forever. This includes faxes, which are stored electronically in the Feith document database. This is due to the unique nature of the system’s mission to memorialize Veterans.

Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers. All VA personnel responsible for these activities must complete annual cybersecurity and privacy awareness training. permits destruction) by shredding or similar VA approved methods in accordance with VA Directive.
3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research? This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII collected by MBS is not used for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of Information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

_Principle of Minimization_: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

_Principle of Data Quality and Integrity_: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:** There is a risk that the archived data may be retained longer than necessary. Records, especially those containing Personally Identifiable Information (PII) or Sensitive Personal Information (SPI) that are retained longer than required are at a greater risk of unauthorized access, privacy or security breach. This also increases the risk that an individual's information may be accessed by those without a need-to-know.
**Mitigation:** The National Archives and Records Administration (NARA) will dispose of records in accordance with NARA’s guidelines therefore information will only be kept in compliance with VA RCS10-1.
Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted? Note: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

*Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.*

*State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.*

*For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.*

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

**Data Shared with Internal Organizations**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
</table>
| AITC - Master Person Index (MPI) via VA Authentication Federation Infrastructure (VAAFI) | Verifies and updates MEL record when Updated in the MBS (BOSS/AMAS) | Date of Birth  
Date of Death  
Gender Code  
Veteran ID  
Relationship Code  
Name  
Social Security Number | Encrypted using a web service from server (MBS-QITC) to server (MPI-AITC): sent to |
<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memorial Enterprise Letters (MEL)</td>
<td>MEL pulls the Veteran case data from AMAS to generate a new letter, also updates AMAS with the completed letter and letter status.</td>
<td>Decedent name, Veteran ID, spouse name, cemetery, country, SSN, monument ID, case status, discharge type, service number, monument type and description, war awards, date of birth, date of death, branch, rank, date entered on duty, date released from active duty, date case established.</td>
<td>A database queue by Oracle triggers; MVI (web service program) picks up the data from the database queue</td>
</tr>
<tr>
<td>Memorial Enterprise FAX Service Re-Platforming (MEFSR)</td>
<td>Applications for Memorial benefits, such as VA FORM 40-1330, VA FORM 40-1330M, or VA FORM 40-0247, are along with any supporting documentation (e.g. DD Form 214), to NCA for processing via the EFSR system. EFSR sends PII internally, in non-identifiable form through secure digital faxes, to the MBS-BOSS Feith document database.</td>
<td>Decedent name, Veteran ID, spouse name, cemetery, country, SSN, monument ID, case status, discharge type, service number, monument type and description, war awards, date of birth, date of death, branch, rank, date entered on duty, date released from active duty.</td>
<td>Secure faxes are sent via an encrypted connection within the VA network.</td>
</tr>
</tbody>
</table>

Java Database Connectivity (JDBC)
<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFTP Server - Accessed by NCA Users with approved access authorizations (VA Form 9957) on file; NCA users log in/download the file as needed to update the GovDelivery e-mail list of funeral home contacts.</td>
<td>A cron job called “ncso-listbuilder” extracts BOSS funeral home contact e-mail addresses and posts the output report to the SFTP Server for approved users to access for NCA authorized business purposes.</td>
<td>Email addresses for funeral home points of contact.</td>
<td>SFTP comma-separated values (CSV) file</td>
</tr>
<tr>
<td>Memorial Benefits Management System (MBMS)</td>
<td>Provide a replacement for the Burial Operations Support System Enterprise (BOSS-E) by replacing BOSS-E’s sub-applications with a more cohesive enterprise system while incorporating new functionality and process improvement. Implemented through a series of successive builds that will provide continuous improvements in functionality while moving users off the legacy systems and culminate with BOSS-E’s decommissioning. Provides an increase in benefits delivery efficiency to Veterans and their families by</td>
<td>Veteran ID, Decedent or Veteran Name, SSN, Date of Death, Date of Birth, Gender Code, Relationship Code, home of record, spouse name, cemetery, country, case status, discharge type, service number, war awards, branch, rank, date entered on duty, date released from active, NOK information/address, monument ID, monument type and description, spouse information, email addresses for funeral home points of contact.</td>
<td>Direct database connection from the MBMS to BOSS/AMAS.</td>
</tr>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of the information being shared/received with the specified program office or IT system</strong></td>
<td><strong>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</strong></td>
<td><strong>Describe the method of transmittal</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>improving access to benefits tracking and delivery, enhancing end-user functionality to the system, and providing increased customer service satisfaction through shorter processing times. Connection is required between BOSS and the MBMS to support the entire memorials case lifecycle: Time of need cases will be established in the MBMS leveraging legacy data in BOSS for case validation. Once the case manager has conducted eligibility and completed scheduling of the internment, the case will be transferred to the BOSS system for downstream processing and reporting.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.2 PRIVACY IMPACT ASSESSMENT: Internal Sharing and Disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

**Privacy Risk:** The privacy risk associated with maintaining SPI is that this data may be disclosed to individuals who do not require access, which would increase the risk of the information being misused.
**Mitigation:** The principle of need-to-know is strictly adhered to by the MBS (BOSS/AMAS) personnel. Only personnel with a clear business purpose are allowed access to the system and to the information contained within.
Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), a Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties.
### Data Shared with External Organizations

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### 5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

**Privacy Risk:** Not applicable, as there is no sharing of information outside of NCA or VA with external agencies.

**Mitigation:** Not applicable, as there is no sharing of information outside of NCA or VA with external agencies.
Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Individuals are notified of collection information via the SORN published in the Federal Register (48VA40B) and via the respondent burden cited on relevant forms. Below are the links to the various forms.


6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

Responding to collection is voluntary; however, if information is not provided; then benefits may be denied.
6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

This question is related to privacy control IP-1, Consent.

Responding to collection is voluntary; therefore, consent of use is not applicable.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

**Principle of Transparency:** Has sufficient notice been provided to the individual?

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

**Privacy Risk:** There is a risk that members of the public may not know that the Memorial Benefits System exists within the VA.

**Mitigation:** VA mitigates this risk by providing the public with two forms of notice that the system exists; the Privacy Impact Assessment and the System of Record Notice.
Section 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Information collected in BOSS/AMAS can be accessed under the FOIA and Privacy Act regulations; Title 5, U.S. Code subsection 552 and Title 5, U.S. Code subsection 552a. Records can be requested electronically at ncafoia@va.gov or contacting NCA FOIA Officer, Nikki Benns, at Nikki.Benns@va.gov.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Requests for records can be submitted electronically at ncafoia@va.gov or by contacting NCA FOIA Officer, Nikki Benns, at Nikki.Benns@va.gov.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that
even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are notified of procedures for correcting their information via SORN published in the Federal Register (SORN 48VA40B).

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Individuals are notified of procedures for correcting their information via SORN published in the Federal Register (SORN 48VA40B).

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.
Follow the format below:

**Privacy Risk:** There is a risk that the individual accidentally provides incorrect information in their correspondence.

**Mitigation:** Before entering data into the BOSS/AMAS components of MBS, data are manually verified and cross referenced against available information on DoD Form 214. Since the information is submitted directly from an individual, the information may be validated with the original source.
Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

*Describe the process by which an individual receives access to the system.*

*Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

*Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

NCA Business Systems Division at the QITC (a component of the Infrastructure Operations Health, Benefits, Memorial and Corporate Support Pillar) manages BOSS/AMAS application accounts. All personnel in this division are required to complete additional role-based training prior to gaining database or system administrator access. All requests for accounts require submission of VA Form 9957 and are made through the Enterprise Service Desk ticketing tool which logs/tracks the request. The ticket and 9957 (approved by the supervisor) is routed to the QITC Application Support Group under NCA Business Systems Division. NCA Business Systems Division personnel follow formal Account Management procedures for creating, modifying, disabling and removing user accounts. Through the Oracle database, the DBAs can report on the status of accounts in real-time. Accounts are automatically set to disable after a period of 90 days of inactivity.

NCA follows Access Control policy as prescribed for VA Enterprise in VA Directive and Handbook 6500. Only VA personnel may access VA-owned equipment used to process VA information or access VA processing services. Employees and contractors may not share with non-VA employees or unauthorized personnel instruction or information regarding how to establish connections with VA private networks and computers. Personnel may not share remote access logon IDs, passwords, or other authentication means used specifically to protect VA information or access techniques to VA private networks.

VA information systems utilize Group Policy Objects (GPO) to manage Active Directory accounts. GPOs consist of a set of rules which control the working environment of user accounts and computer accounts. The GPOs provide the centralized management and configuration of operating systems, applications and users' settings in an Active Directory environment. The GPO restricts certain actions that may pose potential security risks.

User accounts are reviewed on a quarterly basis and disabled after 90 days of inactivity. User account requests are approved by the user’s supervisor or the contracting officer technical representative (COTR). General user and administrative Windows accounts are managed through Active Directory.
8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, a Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If yes, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, VA contractors can have access to BOSS/AMAS. VA contract employee access is verified through authorized VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

Yes, VA contractors can have access to BOSS/AMAS. VA contract employee access is verified through authorized VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

If No or In Process, provide your **Initial Operating Capability (IOC) date**: June 20, 2022

The FIPS 199 classification of the system (MODERATE).
Section 9. Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

The System is being hosted in VAEC AWS.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=853&FType=2:

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract).

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?
This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. The RPA may also be referred to as “Bots” or Artificial Intelligence (AI).
Section 10. References

Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Authority and Purpose</td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td>Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td>Data Minimization and Retention</td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td>Individual Participation and Redress</td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td>Security</td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td>Transparency</td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td>Use Limitation</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

LAKISHA V WRIGHT 111646
Digitally signed by LAKISHA V WRIGHT 111646
Date: 2022.03.10 08:44:14 -05'00'

Privacy Officer, Lakisha Wright

Karen A. McQuaid 321576
Digitally signed by Karen A. McQuaid 321576
Date: 2022.03.10 07:59:28 -06'00'

Information Systems Security Officer, Karen McQuaid

Michael S. Ouslander 523383
Digitally signed by Michael S. Ouslander 523383
Date: 2022.03.10 08:53:24 -05'00'

Information Systems Owner, Michael Ouslander
Appendix A-6.1

Provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).


https://vaww.va.gov/vaforms/va/pdf/VA40-1330M.pdf